ON SECURITY AND PERFORMANCE IN ECC, NONCOMMUTATIVE CRYPTOGRAPHY AND SIGNCRYPTION

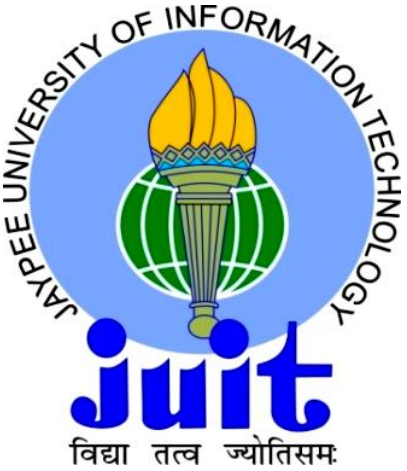
Synopsis submitted in partial fulfillment for the Degree of

DOCTOR OF PHILOSOPHY

By

GAUTAM KUMAR

Enrollment No. 136202



Under the supervision of

Dr. Hemraj Saini

Department of Computer Science and Engineering

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

February, 2017

ABSTRACT

The synopsis addresses the security and performance advancements for the Discrete Logarithmic Problem (DLP) in the primitives of cryptography such as: Elliptic Curve Cryptography (ECC), Edwards and twisted Edwards Curves, Noncommutative Cryptography (NCC), multilayer key generation for ECC using signcryption and proxy re-cryptographic approach. These primitives formulates into the following five objectives:

The first objective claims Radix-16 scalar multiplication without pre-computations for ECC. Using the designed hardware support, the proposed approach shows the more appropriateness for reduced instruction set computing which is particularly suitable for low memory devices along with resistance to the simple side channel attack and safe-error fault attack. The theoretical computation is 6.25 percent faster than the recently proposed Radix-8 scalar conversion technique without pre-computed operations. The performance from the hardware perspective is also improved by 8.33 percent.

The second objective works on the architecture of prime Edwards curves and extended Twisted Edwards curves on 4-processors and 8-processors to obtain the parallelization of intermediate operations. The proposed scalar multiplication results for both the curves in reduced clock cycles and multiplication processing costs.

The third objective pertains on Noncommutative Cryptography (NCC), which is truly a fascinating area with great hope of advancing performance and security for high end applications to provide a high level of safety measures. The basis of this group is established on the Hidden subgroup or subfield problem (HSP). The proposed scheme is based on the extra special group (ESG) to find the solution of an open problem of Noncommutative cryptographic platform. ESG supports at Heisenberg, Dihedral order and Quaternion group. The working principle is made possible on the random polynomials chosen by the communicating parties for secure key-exchange, encryption-decryption and authentication schemes using NCC. The proposed scheme enhances the computation from the general group elements to equivalent ring elements, known by the monomials generations for the cryptographic schemes. The applied group of orders for the computations is more challenging for length based attacks and brute-force attacks.

The fourth objective is the key generation for multilayer consensus using the signcryption approach where, signcryption combines signature and encryption cost in the form of reduced computation and communication cost in a single step. The proposed methodology significantly reduces the overall computation time in key generation and signature generation process. The proposed algorithm is verified and validated using SPAN and Automated Validation of Internet Security Protocol Architecture (AVISPA) tools for certain parameters to ensure its integrity and safety.

The fifth objective focuses on situations under a cryptographic key management by a semi-trusted proxy, where data encrypted under one cryptographic key need to be re-encrypted. In modern era of cryptography, this is one of the new diverse trends and motivating issue. It is a secure and efficient trust based approach for third party like proxy which is not directly involved in the communication process. The same work is verified and validated on AVISPA/SPAN to ensure its integrity and safety. In addition, the proposed Radix-16 scalar multiplication approach is validated using a telemedicine scenario.

Table of Contents

	PAGE NO.
ABSTRACT	i-ii
1. INTRODUCTION	1-3
2. OBJECTIVES AND CONTRIBUTIONS	4-10
2.1 Radix-16 Scalar Multiplication without Precomputation	4
2.2 Parallelization of Edwards Curve & Twisted Edwards Curves	5
2.3 Novel Noncommutative Cryptography Scheme Using Extra Special Group	8
2.4 Secured ECC-PAKE Protocol for Multilayer Consensus using Signcryption	9
2.5 Signcryption Re-Cryptography and Telemedicine Application on Radix-8	9
3. CONCLUSION AND FUTURE WORK	11
4. REFERENCES	12-15
5. LIST OF PUBLICATIONS	16-17

1. INTRODUCTION

The foundation of cryptography is conceptually a centralized approach to generate the randomness and unpredictable behaviors of keys. The management and maintenance of associated resources used in cryptographic process in order to provide a secure communication in the existing environment [1, 2]. Cryptography is closely connected to number theory where the secrecy relies on probability theory and analysis of cipher systems. The securities of these schemes are based on the presumed difficulty of a number theoretic problem. A number theoretic foundation offers a framework for many cryptographic systems that provides most of the hard computational problems to ensure security [3]. Most key agreement protocols rely on the difficulty of a class of number theoretic problems generally combines under the term discrete logarithm problem. Construction of secure systems is possible with the use of information theoretical designation where mathematical models and proofs ensure the foundation of security and performance issues where in general the use of combinatorial structures and algebraic codes are considered as the main techniques [4, 5].

The acceleration of cryptographic function progresses by identifying sensitive data and determining the level of required encryption which is considered as one of the research gaps [6]. The establishment of the key lengths with the right combination of flexibility and protection is the widely acceptable to most of the standards that is analogous with the strong classification on ciphers which changes over specific time duration [7]. The protection to control the sensitive data is the suite of encryption schemes that enables it to expand in the volumes, location and types from the data centers in virtual environments. A dedicated hardware is used to provide a variety of solutions for online or offline cryptographic processes for the application servers that needs to provide the reduced or efficient computational complexity [8].

The efficiency of algorithm in many public key cryptosystems relies on the speed of the arithmetic in various algebraic structures, such as finite field operations or adding points on an elliptic curve [9, 10]. It is important to work improving the speed of the underlying arithmetic operations along with the efficient solutions in arithmetic of computational number theory.

Scalar multiplication in Elliptic curve cryptography (ECC) [11, 12] is a fascinating area with great hope of advancing performance and security for high end applications. On account of the identified research gaps and motivations our proposed work is based on scalar multiplication

without pre-computed operations for ECC which is computationally faster than all the existing scalar multiplication approaches along with marginal improvements in hardware performance. The proposed phenomenon, computationally faster along with no pre-computations, is more appropriate for reduced instruction set computing and particularly suited for low memory devices with resistance to the simple side channel attack and safe-error fault attack.

Further, the scalar multiplication work is based on Edward's curve [13] and twisted Edwards curve [14] with significant overall improvement. The Edwards curves are one of the cryptographic forms of advanced study for generating the more randomness and unpredictabile behaviors. A numbers of researches have shown the significant improvements to solve the above issues over two, four and eight processors to immensely the contribution in the field of security. In the proposed approach, the same methodology is applied on four and eight processors to show the advancement in performance on input scalar (usually secret key) which multiplies with point-coordinates on curve.

Moreover, Noncommutative cryptography is considered as a special case for scalar multiplication in the field of cryptography for upcoming future security [15, 16, 17, 18]. It is truly a fascinating area with great hope of advancements in performance and security where the Hidden subgroup or subfield problem (HSP) can be used as the basis of cryptography. The working principle is based on the random polynomials chosen by the communicating parties to secure key-exchange, encryption-decryption and authentication schemes on NCC. In this regard, group, ring, field, algebraic structures or special or peculiar matrices have shown the potential advantages to be used in this approach.

In addition, signcryption [19, 20] is one of the approach that is redundant in terms of bandwidth consumption and usage of computational resources which logically combines with the individual signature and encryption cost in the form of a single stride of operation. The proxy Re-cryptography proposes due to key escrow problem that has suffered in the public key infrastructure (PKI) for generating and maintaining the public keys for the distribution of certificate. In the escrow problem, during the key exchange process, a secret key is stored by the third party where if proper precautions are not taken in to the consideration, the same key can be compromised or the original user(s) information is lost by the intruders. This directs us towards a probably secure and efficient approach regarding the trust based problem for third party which is

not directly involved ‘called proxy’, can be solved by using signcryption re-cryptographic approach.

In the end, an application oriented work for Telemedicine [21, 22] using ECC is presented on robust application for reduced computational complexity. The methodology is applied on Scalar Multiplication without precomputation for Radix-8. This approach provides a motivation to offer a path on an area of ECC which uses a smaller key size will be applicable for all other applications on a same level of security strength with faster computations.

2. OBJECTIVES AND CONTRIBUTIONS

Computational efficiency of scalar multiplication for Elliptic Curve Cryptography (ECC) can be enhanced by reducing the required addition and doubling operations.

2.1 Radix-16 Scalar Multiplication without Precomputation

Motivation: From the research point of view, a number of procedures/algorithms have been applied, where the major consideration is in reducing the precomputed operations. The procedure for scalar multiplication $(\mathrm{Q} = \mathrm{kP})$ is based on secret key k on prime field p on Elliptic E designed(a, b), $\mathrm{E_p}(\mathrm{a}, \mathrm{b})$, and the key should be less than its chosen prime p. It is easy to calculate Q from k and P, but it is relatively hard to determine k on the given P and Q. For elliptic curve, this is known by discrete logarithm problem (DLP). According to the definition of ECC, scalar multiplication is based on point addition (ADDs) and point doubling (DBLs) operations, where for one point ADDs and for one point DBLs requires pre-computed operations are 13,617 and 14,000 clock cycles [23]. The complexity of existing algorithms is presented in table 1 in terms of number of addition and doubling operations. In the table-1 the key is of k words for all the existing algorithms.

Table 1: Algorithms Complexities for Scalar Multiplication

Algorithm	**Complexity**
Most Significant Bit	k DBLs & $k/_2$ ADDs
Least Significant Bit	$k/_2$ DBLs & $k/_2$ ADDs
Montgomery Method	k DBLs & k ADDs + Side Channel Attack
Non-Adjacent Form (NAF)	$k/_2$ DBLs & $k/_2$ ADDs + Side Channel Attack
Window methods	$k/_{(w+1)}$ ADDs
Sliding window method	Escaping series of zero's on $k/_{(w+1)}$ ADDs
Radix-8 without Pre-Computations	$log_8^{(k+1)}$ without (ADDs & DBLs)

For Elliptic Curve Scalar Multiplication a new algorithm is proposed in 2015 by Abdulrahman & Reyhani-Masoleh [24] on the basis of Radix 8 without pre-computed operations, with no addition and doubling operations. This is reported to be one of the most optimized & reduced complexity on $log_8^{(k+1)}$ for this scheme. This is also enhancing the parallelism in the arithmetic

field and point arithmetic operations. The above existing approaches are representing the research gap on the reduced complexity for scalar multiplication.

Contribution: In order to overcome the mentioned limitation, we have proposed a secure and efficient scheme for Elliptic curve scalar multiplication on Radix-16. The potential contributions of the proposed mechanism are summarized as follows:

(i) It claims Radix-16 scalar multiplication without pre-computed operations for ECC in the field of Cryptography.

(ii) It is theoretically computing 6.25 percent faster than the recently proposed Radix-8 scalar conversion method.

(iii) The hardware performance also gets improved by 8.33 percent.

(iv) The computational complexity for the proposed algorithm is stronger, secure, and efficient for scalar multiplication using ECC.

(v) The time complexity is in the order of $\log_{16}(k+1)$ and it is to the more appropriate for reduced instruction set computing.

(vi) The suitable future scope of proposed algorithm is to implement it for low memory devices.

Above contributions are achieved by using the support of hardware as depicted in figure 1. The overall dependency graph of figure 1 is depicted in figure 2.

2.2 Parallelization of Edwards Curve & Twisted Edwards Curves

Motivation: The sub-section 2.1 is based on ECC with 2-point multiplication which can be further extended by the twists created by Edward's curves and extended Twisted Edwards curves to improve the parallelization of operations.

Contribution: Prime based Edwards curve & extended Twisted Edwards curves [25] works for scalar multiplication on 4 and 8 processors.

The specific contribution is summarized as follows:

(i) The Edwards Curves and twisted Edwards Curves problems on four and eight processors solves are the same but on reduced computation cost from $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ on four processors and $2M + 3A$ to $2M + 2A$ on 8-processors, respectively. This has accumulated on reduced clock cycles with resistance to the simple side channel attack.

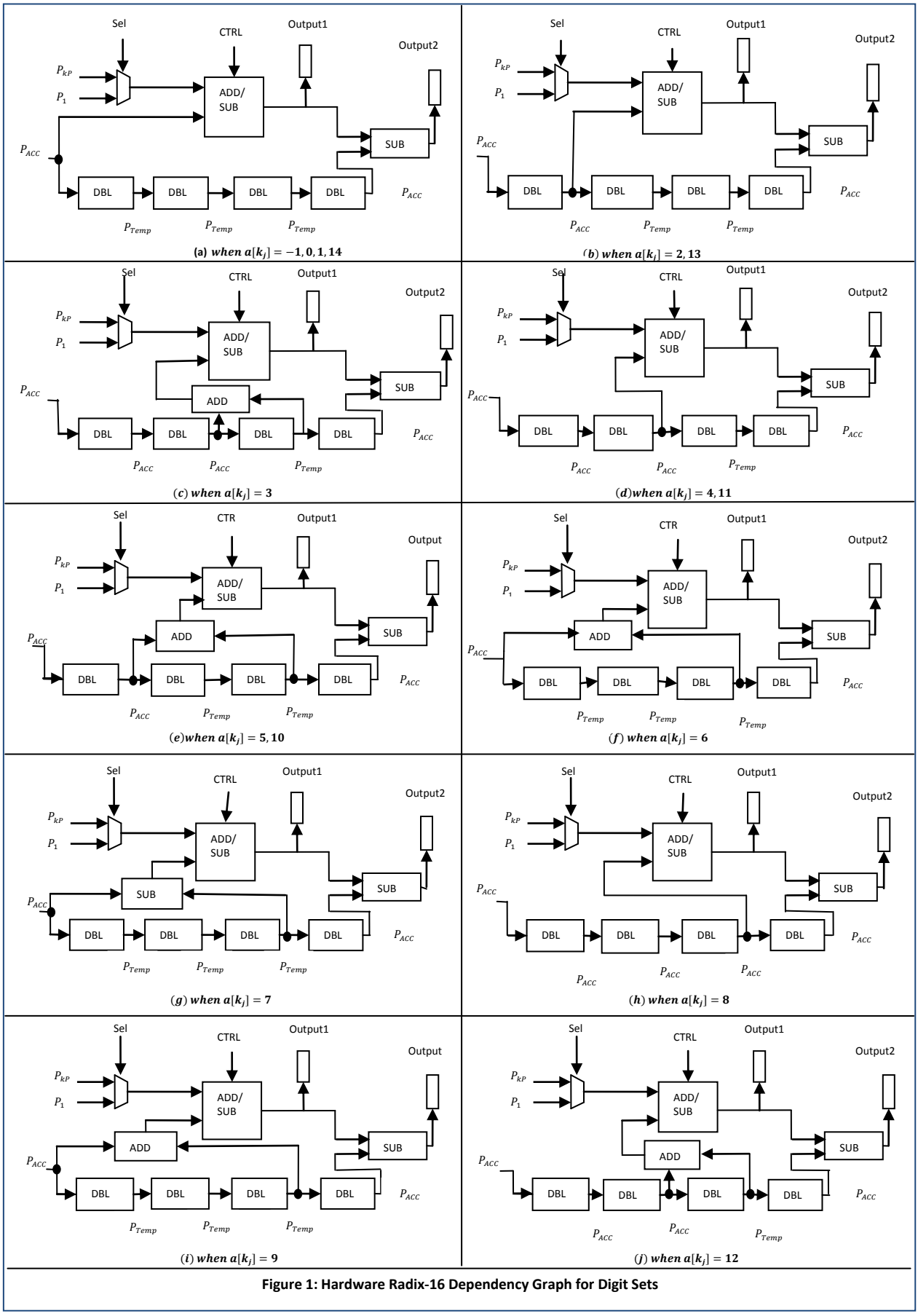


Figure 1: Hardware Radix-16 Dependency Graph for Digit Sets

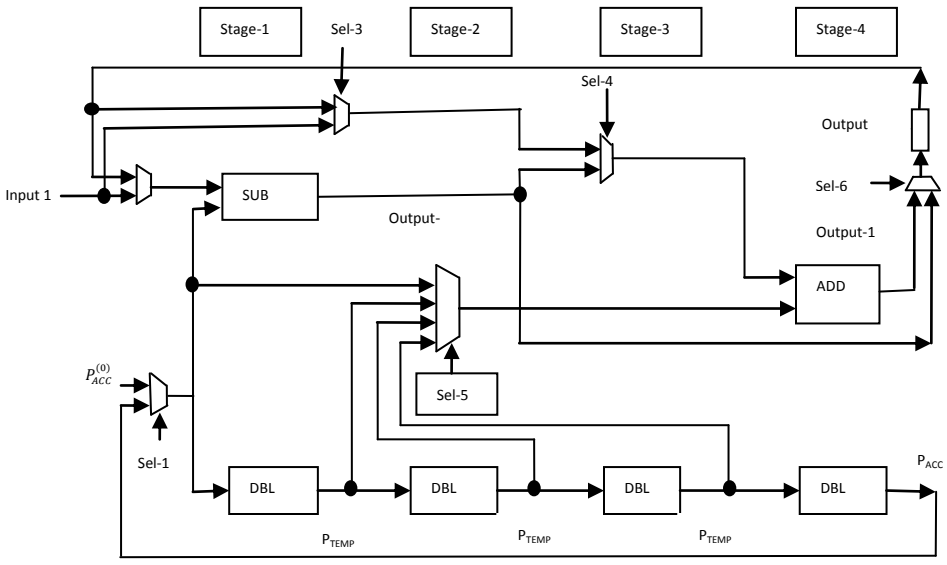


Figure 2: Overall Dependency Graph

(ii) A generalization of scalar multiplication for s-bit scalar requires $6\frac{(s-1)}{3}M + 3\frac{(s-1)}{3}A$ according to the Montgomery Ladder method in [15] and the extended twisted Edwards curves on radix-8 ECSM method requires $5\frac{(s)}{3}M + \frac{(s)}{3}A$ in [13]. Here, our proposals for scalar multiplication requires operations on $4\frac{(s)}{3}M + \frac{(s)}{3}A$, is reporting a big advancement cost for size of multiplication. The figure 3 represents the significant of contribution with improved reduced multiplication costs.

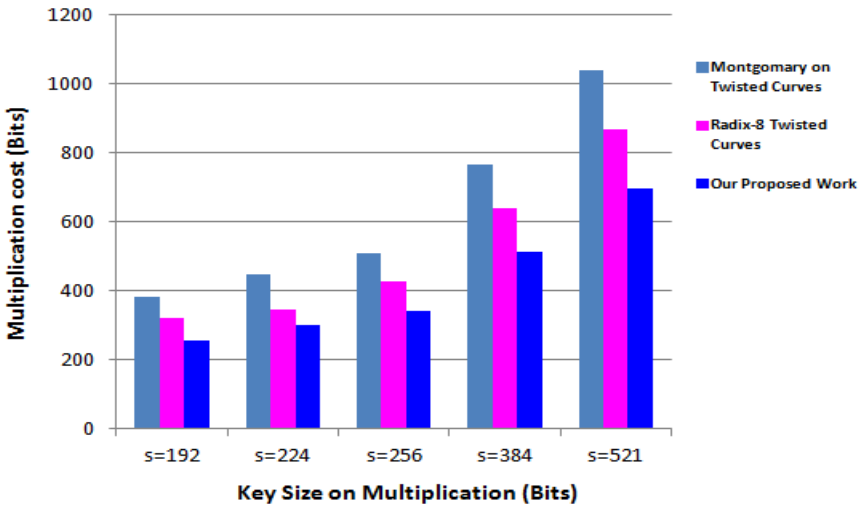


Figure 3: Comparative cost reduction on multiplication

2.3 Novel Noncommutative Regular Cryptography Scheme Using Extra Special Group

Motivation: The various open research problems and a new direction of future security to uncover through Non-Commutative cryptography (NCC) [26, 27, 28]. This has enhanced from the general group elements to equivalent substituted elements, known by the monomials generations for the cryptographic schemes. The group of orders is more challenging to assail like length based attack, automorphism, and brute-force attacks. However, to improve the performance using less memory, avoiding repetitions in process, look-ahead for future security, automorphism attacks and alternative solutions during the computation process adds to the big advantage in this field of cryptography. The proposed security assumptions are intractable by the adversary and the attacks like length based, brute-force, automorphism, being negligible to revert back to the original information.

The issue related to the ring structure of the group elements is one of the most motivational concerns. A typical semi-ring structure, such as sparse matrices, showed the potential advantages towards a possible way to avoid the various attacks. The initial order for general and monomials [original parameters are hidden, and it's probably equivalent participated in computation] structure on polynomial $\mathbb{Z}$-modular Noncommutative is the foundation, that is based on dihedral order 6 in a three dimensional matrix rings.

Contribution: We identified the behavior of Extra Special Group and applied in cryptographic scheme which provides more robustness and unpredictability as compared to all known schemes of Non-Commutative cryptography. The overall contribution is summarized as below:

(i) A cryptographic protocol is derived using multidisciplinary scenario of Extra Special Group which is more resistant to the length based attacks and side channel attacks and works on the bigger range of probabilistic theory through random polynomial generation for the communicating parties.

(ii) Designed the mono-morphism group or ring element for minimum order of this group.

2.4 Secured ECC-PAKE Protocol for Multilayer Consensus using Signcryption

Motivation: Signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logical single step which is lower in cost. The discrete algorithm problem on signcryption cost is 58% less in average computation time and 70.3% less in average communicational overhead. The current status says that the existing algorithms need to signcrypt the message with each of its intended recipient's public keys and send them separately to each one of them. The motivation for proposed approach is to reduce the bandwidth consumption and computational resource usage [29-33] along with the removal of Escrow problem.

Contribution: The major points of the contribution are as below:

(i) A methodological approach is presented on protocol generation for a better, improved and stronger security on reduced costs. The basic primitives are applied on Diffie-Hellman and Elliptic Curve Cryptography whose purpose is to provide the security properties for protocol compositional logic by focusing on privacy rights in information assessment in multidisciplinary obligations.

(ii) We portrait a signcryption approach for password authenticated key exchange protocol for multilayer consensus which logically combines individual signature and encryption cost in the form of reduced computational and communications cost in single stride of operation. The overall computation time potentially reduces for the proposed methodology on key generation and signature.

(iii) The results for ECC based multilayer consensus key generation approach are tested on Automated Validation of Internet Security Protocol Architecture (AVISPA) tool and SPAN tool.

(iv) Further, by preserving the definition of signcryption, we enhanced the same scheme in relations to the other proposed schemes.

2.5 Signcryption Re-Cryptography and Telemedicine Application on Radix-8

Motivation: The proxy Re-cryptography has been proposed due to key escrow problem that has suffered in the public key infrastructure (PKI) for generating and maintaining the public keys for certificates distribution [34-36]. In key Escrow problem, during the key exchange process, a secret key is stored by the third party in which if proper precautions are not taken in to consideration, the same key is compromised or original user(s) information is lost. The encrypted matter may be used to decrypt, and/or is allowing restoration of the primary matter to its

unencrypted state. So in some way the third party involved is risky in escrow systems. The key escrow also enables to provide a backup source from cryptographic keys. Where the modern cryptography is focusing on to solve the trust problem using the proxy re-cryptographic primitive as an interdisciplinary approach of computer science. A combined effort by Blaze, Bleumer, and Strauss in 1998 has gained the credit in the idea of proxy re-cryptography that has been further formalized by Ateniese and Hohenberger in 2005, -which consists of two methods such as: proxy re-encryption and proxy re-signature. The goal of proxy re-encryption is to securely enable the re-encryption of cipher texts from one key to another without relying on honest parties. Similarly, the goal of proxy re-signature is to securely enable the signature signed by one to transform a duly signed message without relying on trustworthy parties. An enhanced proxy re-signature scheme has been proposed in 2006 and also discussed its several potential applications related to the same. It has been predicted that proxy re-encryption and proxy re-signature will play an important role. Since then, researchers have been sparked to light light in this area. That's why some excellent schemes have been proposed, like the IEEE P1363.3 standardization group is establishing the standard for proxy re-encryption which will certainly give power for researching in the field of proxy re-cryptography [3]. A semi-trusted is an entity to convert cipher texts addressed to those that can be decrypted by using some special information.

Contribution 5:

(i) In this a more optimized notion of signcryption with proxy re-cryptographic and its formal verification is presented.

(ii) It is an innovative approach in the modern cryptography which works in two parts such as proxy re-encryption and proxy re-signature where a semi-trusted proxy can translate a ciphertext to another ciphertext for the same plaintext using encryption and signature algorithms.

(iii) Further the prposed mechanism presents an application oriented work for Telemedicine using ECC without precomputation on Radix-8 scalar multiplication. The reason to cover this problem is to provide a path on a fascinating area of ECC on a smaller key size that will be applicable for all applications on same level of security strengths.

3. CONCLUSION AND FUTURE WORK

The proposed Radix-16 algorithm is contributing its benefits for short memory device on low computation costs. The future scope of the proposed objective is still to make an improvement over the worked done for related to simple constructs of instruction sets to execute much faster within the CPU or as often without having to use memory. Again, twists in ECC on Edward's curves and Extended Twisted Edwards curves for four and eight processors are solved and are reporting a marginal enhancement on reduced multiplication costs.

Further, the new era's advancements are mostly looking up, with stronger security in connection with the Noncommutative cryptography on Extra Special Group. The proposed solution is strongly meeting this challenge with the security enhancement for any applications using the non-commutative properties.

In relation to the proposed approaches a signcryption and proxy re-cryptography primitives adds on an additional to ECC and adds a better applicability on reduced costs in the field of cryptography. A validation for Telemedicine application on AVISPA and SPAN justifies our used strategies.

4. REFERENCES

[1] Oded Goldreich, "Foundations of Cryptography Basic Tools," Vol. 1, Cambridge University Press, UK, 2004

[2] Oded Goldreich, "Foundations of Cryptography Basic Applications," Vol. 2, Cambridge University Press, UK, 2009

[3] W. Diffie and M. E. Hellman, "Privacy and authentication: An introduction to cryptography," Proc. IEEE, 67, 397–427, March 1979.

[4] J. Baek, "Construction and Formal Security Analysis of Cryptographic Schemes in the Public Key Setting," PhD Thesis, Monash University, 2004

[5] Kevin S. McCurley, "The Discrete Logarithm Problem," Proceedings of Symposia in Applied Mathematics, Vol. 42, pp. 49-74, 1990.
[Online: http://www.mccurley.org/papers/dlog.pdf]

[6] A. Joux, A. Odlyzko, C. Pierrot, "The Past, evolving Present and Future of Discrete Logarithm" Open Problems in Mathematics and Computational Science, Springer International Publishing, pp 5-36, 2014. DOI: 10.1007/978-3-319-10683-0_2

[7] A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance" Advances in Cryptology: Proceedings of EUROCRYPT 84, ACM Digital Library, pp. 224–314, 1985.

[8] V. Jirasek, "Practical Application of Information Security Models," Information Security Technical Report, vol. 17, Issues 1–2, pp. 1-8, Feb. 2012. DOI: 10.1016/j.istr.2011.12.004

[9] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory, vol. 22, No. 6, pp. 644-654, Nov. 1976.
DOI: 10.1109/TIT.1976.1055638

[10] K. Jarvinen and J. Skytta, "Parallelization of High-Speed processor for Elliptic Curve Cryptography," IEEE Transaction on VLSI, vol. 16, No. 9, pp. 1162-1175, Sep. 2008.

[11] N. Koblitz, "Elliptic Curve Cryptosystems," Math Computation, vol. 48, No. 177, pp. 203-209, 1987.

[12] V.S. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology, pp. 417-426, 1986. DOI: 10.1007/3-540-39799-X_31

[13] H.M. Edwards, A Normal Form of Elliptic Curves, Bulletin American Mathematical Society, vol. 44 (July 2009), No. 3, pp. 339-442.

[14] H. Hisil, K. K. H. Wong, G. Carter, and E. Dawson, "Twisted Edwards curves Revisited," Lecture Notes in Computer Science, vol. 5350, pp. 326-343, 2008. DOI: 10.1007/978-3-540-89255-7_20

[15] I. Anshel, M. Anshel, and D. Goldfeld, "Non-abelian key agreement protocols," Discrete Applied Mathematics. Elsevier, Vol. 130(Aug 2003), pp. 3-12, 2003. DOI: 10.1016/S0166-218X(02)00585-1

[16] K.H. Ko, D. H. Choi, M. S. Cho, and J.W. Lee, "New Signature Scheme using Conjugacy Problem," Cryptology ePrint Archive: Report 2002/168, 2002. DOI: https://eprint.iacr.org/2002/168

[17] J. Hughes and A. Tannenbaum, "Length-Based Attacks for Certain Group Based Encryption Rewriting Systems," Institute for Mathematics and Its Application, 2000.
DOI: http://purl.umn.edu/3443

[18] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, and C. Park, "New Public Key Cryptosystem using Finite Non Abelian Groups," In Proceeding of CRYPTO-2001: J. Kilian (Ed.), LNCS, Springer-Verlag., Germany, Vol. 2139, pp. 470-485, 2001.

[19] Y. Zheng, "Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," in Advances in Cryptology-CRYPTO'97, Lecture Notes in Computer Science, Springer-Verlag, vol. 1294, pp. 165-179, 1997.

[20] J. Baek, R. Steinfeld, and Y. Zheng, "Formal Proofs for the Security of Signcryption," in Public Key Cryptography (PKC 2002), Lecture Notes in Computer Science, Springer-Verlag, vol. 2274, pp. 80-98, 2002.

[21] M. A. Hein, Telemedicine: An Important Force in the Transformation of Healthcare, June 2009 [Online: http://www.trade.gov/td/health/telemedicine_2009.pdf]

[22] : Telemedicine Opportunities and Developments in Members States, Second Global Survey on eHealth, 2010
[Online: http://www.who.int/goe/publications/goe_telemedicine_2010.pdf].

[23] C. H. Gebotys, "Elliptic Curve Cryptography," Security in Embedded Devices, Springer, 2010, pp. 75-109. DOI: 10.1007/978-1-4419-1530-6

[24] E.A.H. Abdurrahman and A. R-Masoleh, "New Regular Radix-8 Scheme for Elliptic Curve Scalar Multiplication without Pre-Computation," IEEE Transaction on Computers, vol. 64, No. 2, pp. 438-451, Feb. 2015. DOI: 10.1109/TC.2013.213

[25] B. Baldwin, R. Mononey, A. Byrne, G. McGuire, A Hardware Analysis of Twisted Edwards Curves for an Elliptic Curve Cryptography, in International Workshop on Application Reconfigeration Computing (2009). [Online: https://eprint.iacr.org/2009/001.pdf]

[26] Zhenfu Cao (Ed.), "Noncommutative Cryptography" in New Directions of Modern Cryptography, CRC Press, 2013.

[27] I. Anshel, M. Anshel, and D. Goldfeld, "Non-abelian key agreement protocols," Discrete Applied Mathematics. Elsevier, Vol. 130(Aug 2003), pp. 3-12, 2003. DOI: 10.1016/S0166-218X(02)00585-1

[28] I. Anshel, M. Anshel, and D. Goldfeld, "A Linear Time Matrix Key Agreement Protocol over Small Finite Fields," AAECC, 2006.
DOI: http://link.springer.com/content/pdf/10.1007/s00200-006-0001-1.pdf

[29] H. Nicanfar and V.C.M Leung, "Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System" IEEE Transactions on Smart Grid, pp. 1-12, 2012.

[30] D. H Seo, and P. Sweeney "Simple authenticated key agreement algorithm" Electronic Letters, Institution of Engineering and technology, vol. 35, pp. 1073–1074, 1999. DOI: 10.1049/el:19990724.

[31] : AVISPA-Automated Validation of Internet Security Protocols [online] Available: http://www.avispa-project.org.

[32] Y. Glouche, T. Genet, O. Heen and O. Courtay "A Security Protocol Animator Tool for AVISPA**"** In *ARTIST2 Workshop on Security Specification and Verification of Embedded Systems*, Pisa, May 2006.

[33] R. Saillard and T. Genet, "CAS+", Institute for Research in Computer Science and Random Systems, March 21, 2011.
[Online: http://www.irisa.fr/celtique/genet/span/CAS_manual.pdf]

[34] G. Ateniese, K. Fu, M. Green, S. Hohenberger, "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage," Proceedings of the 12th Annual Network

and Distributed Systems Security Symposium NDSS'05, San Diego, California, 2005. Available at: http://spar.isi.jhu.edu/~mgreen/proxy.pdf

[35] J. Shao, Z. Cao, "Multiuse unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption," Journal Information Sciences, 206, 83-95, 2012. DOI: dl.acm.org/citation.cfm?id=2228798

[36] Z. Wang, X. Du, Y. Sun, "Group Key Management Scheme of Proxy Re-cryptography for Near Space Network," IEEE Int'l conf., 1-5, 2011.

5. LIST OF PUBLICATIONS

Journal Publications

[1] G. Kumar, and H. Saini, "Novel Non-commutative Cryptography Scheme using Extra Special Group,'' Security and Communication Networks, Wiley, Vol. 2017, Issue 5, pp. 1-21, January 2017. DOI: 10.1155/2017/9036382. [*Major Indexing: Science Citation Index Expanded, SCOPUS, DBLP, Compendex*]

[2] G. Kumar, and H. Saini, "Secure and Robust Telemedicine using ECC on Radix-8 with Formal Verification,'' Journal of Information Security and Privacy, IGI Global Publishing, **[Accepted: 19-Aug-2016]**. [*Major Indexing: SCOPUS, ACM Digital Library, Thompson Reuters, DBLP*]

[3] G. Kumar, and H. Saini, ''Effective Signcryption Approach for Secure Convention for Multilayer Consensus using ECC,'' International Journal of Information Security and its Applications, Science & Engineering Research Support Society, vol. 10, No. 1, pp. 287-306, August 2016. [*Major Indexing: SCOPUS, EICompendex, Emerging SCI*]

[4] G. Kumar, and H. Saini, "Reduced Precomputed Scalar Multiplication Cost for ECC," Contemporary Engineering Sciences, Hikari Ltd.,, vol. 9, No. 18, pp. 897-904, August 2016. [*Major Indexing: SCOPUS, CrossRef, Google Scholar*]

[5] G. Kumar, and H. Saini, "Formal Verification on Signcryption Re-Cryptography: Secure and Efficient Approach towards Trust Problem,'' International Journal of Applied Engineering Research, Research India Publication, vol. 10, No. 24, pp. 44271-44277, Nov. 2015 [*Major Indexing: SCOPUS, Thompson Reuters*]

[6] G. Kumar, and H. Saini, "On Reduced Computation Cost for Edwards and extended Twisted Edwards Curves,'' Indian Journal of Science and Technology, Indian Society for Education

and Environment, Vol. 9, Issue 44, November-2016. DOI: 10.17485/ijst/2016/v9i44/105071. [*Major Indexing: SCOPUS, Thompson Reuters, Index Copernicus, DOAJ*].

Conference Proceedings

[1] G. Kumar, and H. Saini, ‘‘Secure Composition of ECC-PAKE Protocol for Multilayer Consensus using Signcryption,’’ International Conference on Communication Systems and Network Technologies, IEEE Computer Society, pp. 740-745, 2015.

[2] G. Kumar, and H. Saini **“**Secure and Efficient ECC: Radix-16 Scalar Multiplication without Pre-Computation,” International Conference on Big Data and Advanced Wireless Technologies, **ACM Digital Library, New York, USA,** 10 November 2016. **ISBN: 978-1-4503-4779-2**

DOI: http://dx.doi.org/10.1145/3010089.3010105 **[Available Online]**

Book Chapter

[1] G. Kumar, and H. Saini, “Formal Verification on Signcryption Re-Cryptography: Secure and Efficient Approach towards Trust Problem’’ Advanced Engineering Research and Applications, (Eds.) B.S. Ajaykumar and D. Sarkar, ISBN No. 978-93-8443-48-1. **[Accepted: 17 Jan 2017]** [*Major Indexing: Google Scholar, Advanced Science Index, Academia.edu*] **[In Press]**